

EGIDE Scanner de vulnérabilité

Prérequis

- Licence Mercury active
- Licence EGIDE
- La box Egide ou une VM egide configurée sur votre réseau
 - vous pouvez réaliser cette tâche via ce tuto
- Vérifier la présence du dépôt ESIA dans /etc/apt/source.list
 - si vous n'avez pas le dépôt: stable.repository.esia-sa.com, ajouter le dépôt: [Ajout du repot esia](#)

Installation

Ajouter le dépôt Egide pour avoir les dernière CVE

[copy](#)

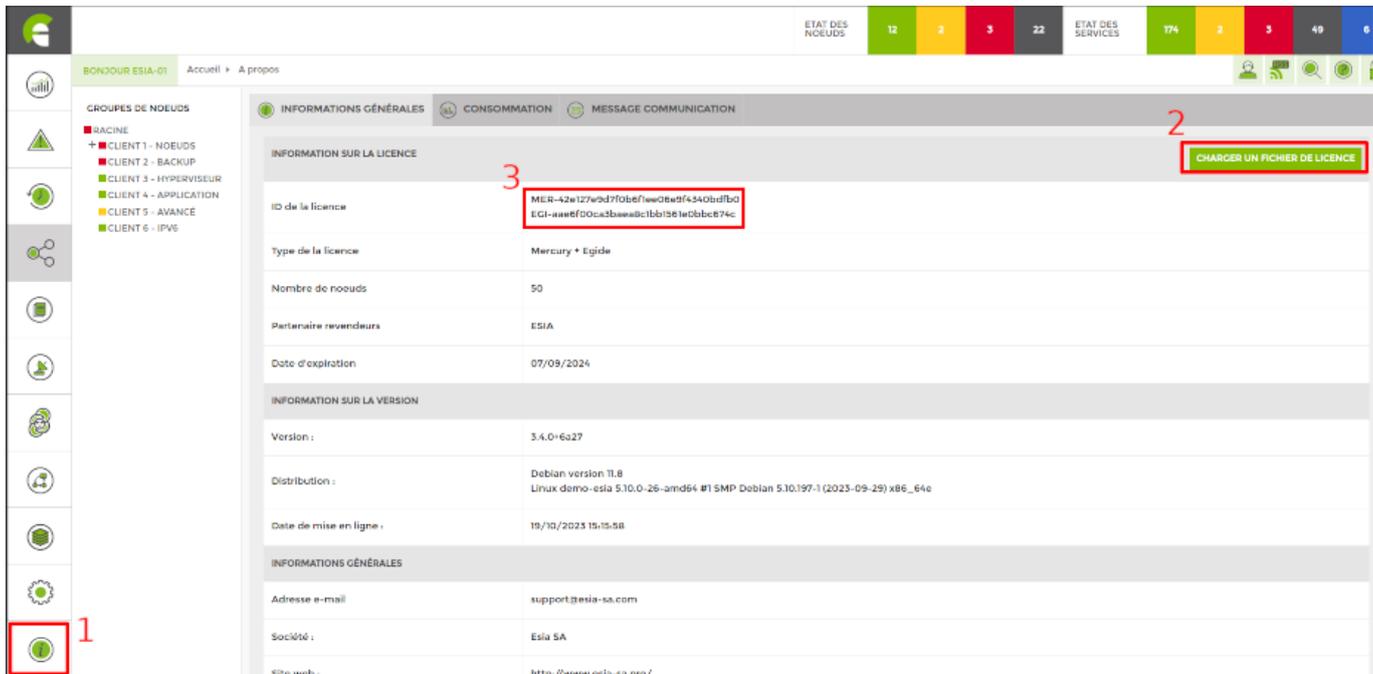
```
echo "deb http://egide.repository.esia-sa.com/egide bullseye
contrib non-free" >> /etc/apt/sources.list
wget -O- "http://egide.repository.esia-sa.com/egide/gnupg.key" |
apt-key add -
```

On peut maintenant installer le web plugin EgideScanner

[copy](#)

```
apt update
apt install esia-webp-egidescan
apt install esia-egide-cve-all
```

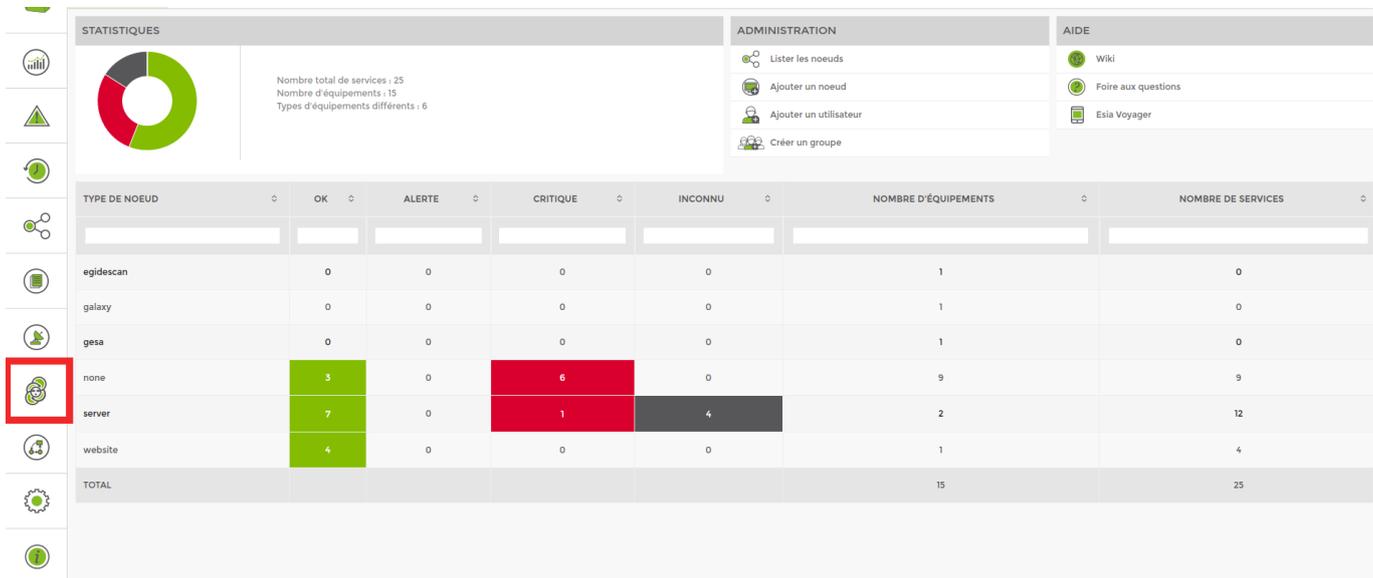
Maintenant allez dans la console WEB de votre Esia pour ajouter la licence EGIDE. Allez dans le menu "A propos" et ensuite cliquez sur "Charger un fichier de licence".



Une fois le fichier chargé, vous devriez voir dans l'ID de la licence une ligne MER-XXXX suivie d'une EGI-XXXX Votre serveur est maintenant près pour la configuration du scanner.

Configuration du scanner

Dans l'interface d'Esia, cliquez sur le menu "Scan Egide".



Veuillez accéder au onglet "Scanner"

The screenshot shows the EGIDE interface with the 'SCANNER' tab selected. The dashboard includes:

- A summary table with columns: Nom (Box_egide), Noeuds (22), Vul. (112), and Status (Scan program).
- A bar chart titled 'SCORES DES SEVERITES' showing the number of vulnerabilities across severity levels from 0-1 to 9-10.
- A table titled 'TOP DES SCORING PONDÉRÉS DES NOEUDS PAR INTERFACE' listing nodes like 'vsvr-nicolas-dev' and '10.12.0.165' with their respective scores and failure counts.
- A table titled 'TOP 10 DES CVE' with columns for ID, DESCRIPTION, STATUS, NOMBRE, SCORE DE BASE, SERVICES, SEVERITÉ, and COMPLEXITÉ.

Cliquez ensuite sur "Ajouter" pour programmer votre scan.

The screenshot shows the 'SCANNER' configuration table and the 'HISTORIQUE DES SCANS' table.

ID	STATUS	GROUPES DE NOEUDS	PRÉCÉDENT SCAN	PROCHAIN SCAN	INTERVALLE	INTERFACE	TYPE	NOM DE LA BOX	ACTION
7	Programmé	groupe_test_bloc_2		2023-10-22 11:00:00	3 heures	ens18_test	DMZ (0,9)	Box_egide	
8	Programmé	groupe_test_bloc_1		2023-10-21 11:15:00	1 jours	ens18_test	DMZ (0,9)	Box_egide	
9	Programmé	groupe_test_bloc_1		2023-10-29 13:15:00	1 jours	ens18_test	DMZ (0,9)	Box_egide	
10	Programmé	groupe_test_bloc_1		2023-10-21 10:00:00	1 jours	ens18_test	DMZ (0,9)	Box_egide	
11	Programmé	groupe_test_bloc_2		2023-11-11 09:00:00	1 jours	ens18_test	DMZ (0,9)	Box_egide	

ID	DÉBUT	FIN	STATUS	INTERFACES	BOX	GRUPE DE NOEUDS	MESSAGE	ACTION
112	2023-05-16 16:40:33	2023-05-16 16:46:09	Terminé	Box_egide	ens18	groupe_test_bloc_2	4 IP addresses (3 hosts up) scanned in 535.91 seconds* exit=""success"	
111	2023-05-16 16:36:47	2023-05-16 16:40:33	Terminé	Box_egide	ens18	groupe_test_bloc_1	2 IP addresses (2 hosts up) scanned in 226.09 seconds* exit=""success"	

Sur la fenetre qui s'apparaitra, veuillez remplir tout les champs

Ajouter SCAN

Sélectionner la box Egide

AJOUT DE SCAN | GESTION DES INTERFACES

Ajouter une interface

INTERFACES AJOUTÉES (CONFIGURÉES)  BOX CONNECTÉE

<input type="checkbox"/>	ID	LABEL	TYPE	NOM LOCAL	ACTION
<input type="checkbox"/>	1	ens18_test	DMZ (0.9)	ens18	 

PARAMÈTRES DU SCAN

Sélectionner les groupes de noeuds

Date de début

DATE ET INTERVALLE DE TEMPS

Intervalle entre scans

Relances en cas d'échecs

Période entre 2 relances (en minutes)

Démarrer

Tout d'abord, il faut ajouter une interface (sur laquelle le scan sera basé) à partir de l'icone encadré en rouge

1. Sélectionner l'interface (parmis ceux que vous avez ajouter)
2. Les groupes de noeuds à scanner
3. La date de début de scan
4. L'intervalle entre les scans

Puis appuyez sur “démarrer”

From:
<http://10.8.0.12/> - **Esia Wiki**

Permanent link:
http://10.8.0.12/interface/module_egidescan

Last update: **2023/10/31 16:49**

